Klay Management Ltd.

Lessons for Successful Business Recovery

White Paper

CONTENTS

1. Preamble

From the seemingly insignificant natural acts that occur halfway across the world, to the ever-present dangers of our new reality, today's integrated organizations are becoming increasingly aware of the spectrum of risks they face. Most have addressed these risks in the form of business continuity plans, and some have been forced to activate these plans in response to disasters that they have faced.

Of course, businesses are more at risk to disruption by mundane issues such as power outages or computer failures. However, these same issues could have effects similar to larger disasters if the organization is unprepared. Lessons can be learned by focusing on significant disasters that have tested some large organizations' abilities to respond.

Today's corporate headquarters act more like financial institutions than the operational head offices of companies 10 or 20 years ago. Distributed, autonomous business units rely on centralized financial, technology, and risk management processes to support their activities. A breach in this central nervous system could be devastating for an unprepared organization.

This paper sets out to discuss several examples of organizations at varying levels of preparedness, and uncover the key messages for executives that are forced to navigate through these uncharted waters.

2. Lessons Learned

2.1. Morgan Stanley

In the aftermath of the tragedy of September 11th, Morgan Stanley was missing seven employees - four of whom had gone back in to make sure everyone was out - and six on-site contract workers. Over thirty-five hundred employees were displaced, and yet Morgan Stanley was back in business when the opening bells sounded once again in the stock markets the following Monday.

Good corporate governance and leadership was responsible for the high level of preparedness that allowed Morgan Stanley to recover its critical functions and restore the company to normal operations as quickly as it did. This was due to advance planning, training of employees, and regular testing to ensure plans were actionable. Most important of all, according to Steven Ruegnitz, Managing Director of Enterprise Applications Security at Morgan Stanley, "Employees at (Morgan Stanley) were empowered ahead of time to take action."[1] Furthermore, "Ruegnitz is convinced that the quick action of leaders saved employees' lives." Exactly one minute after the first plane hit 1 World Trade Centre, Morgan Stanley's security staff began evacuating its 3,528

Corporate Leadership

What Worked: Having a comprehensive plan in place that people understood.

What Failed: Losing four employees because they did not follow the plan.

Key Quote: "Employees at (Morgan Stanley) were empowered ahead of time to take action"

Lesson: Planning and then exercising the plan regularly, ensures people have the ability to adapt under pressure.

[1] Solomon, Melissa (www.computerworld.com)

employees from 2 World Trade Centre, where they were located. Exactly 26 minutes later, senior management had moved to their new command facility. Ten minutes later, their backup system was activated and its New Jersey facilities started buying new IT equipment. These kind of aggressive actions that resulted in lives saved and business losses minimized did not just happen organically. They were the result of careful planning and regular testing and exercising of plans. Most of all, however, they were due to a leadership mentality that valued 'being prepared.'

All of Morgan Stanley's contingency plans – data and application recovery, HR plans, and work area recovery – were clearly laid out and tested on a regular basis, so that when the crisis hit their people knew what to do, despite the trauma and chaos around them. Additionally, senior management was well-versed in the requirements of the plans and what needed to be done, allowing them to make critical decisions quickly and decisively.

Morgan Stanley's contingency plans for their people included the ability to work from home, the provision of grief counselors, aggressive planning to get people back to work earlier, enhanced communications with employees, senior management and the media (including an initiative called "rumour control"), and strategies to deal with temporary housing, transportation and communication.[2]

2.2. Air Canada

On August 15, 2003, Air Canada's operations were thrown into chaos when the backup diesel power generator failed at its Toronto control centre, forcing the airline to ground flights around the world. Due to a major power blackout the day before, Air Canada lost primary power to its Toronto operations control centre. The control centre is where all flight planning is done and keeps track of the location of planes, and crucial information such as weight and fuel for Canada's largest airline.

The impact on customers was extensive as the airline cancelled more than 500 of its 700 scheduled flights. About 50,000 customers were immediately impacted, and passengers at airports around the world grew increasingly frustrated as Air Canada repeatedly pushed back its estimated startup time.

Comprehensive Plans

What Worked: A comprehensive plan including three levels of facilities and power backup.

What Failed: Testing did not adequately confirm backup power reliability and plans did not adequately consider risks to guide decisions.

Lesson: Without tested plans, and appropriate decisions even simple disruptions can affect revenue and reputation.

The secondary power supply to the control centre was activated after the initial blackout, however the backup diesel power generator failed, forcing the airline to shut down the operations centre for a second time, again grounding flights around the world. As a third backup, the airline has a contract that allows the use of an offsite location in the event of an emergency but a decision was made not to use that space because airline officials thought it would be too disruptive and anticipated that the primary power would be quickly restored. By the time Air Canada realized it needed the third backup, the space was no longer available.

[2] Ferris, Gregory J. www.rmmag.com/

The airline asked passengers to stay away from the airports unless they had confirmed their flights, but the airline's call centres seemed submerged by customers' demands. It took days for the airline to operate a normal schedule as it dealt with a backlog of passengers and the logistical nightmare of having aircraft in the wrong cities for startup.

Flights operated by Air Canada's subsidiaries Jazz and Zip, were not as severely affected and were able to resume operations more quickly because they use separate flight control centres operated in different cities.

As a result of this incident, August traffic fell 14%, causing an estimated over $100 Million in losses, and the exposure of Air Canada's vulnerabilities was covered extensively by North American media.

2.3. Royal Bank of Canada

On June 7, 2004 a software programmer updated the source code to a critical program without proper testing. The upgrade contained a programming error, which caused a series of technical glitches that cascaded through the enterprise.

The bad code was entered into the system Monday morning, but had no effect until overnight batches were run. Instead of switching to backup immediately, technical staff worked around the clock to determine the source of the error. By the time they had determined the cause, the backup systems had already inherited the faulty code. The CIO was made aware at 6:00 am on Tuesday. The CEO was noticeably absent during the crisis, causing some reporters to question how much importance senior management placed on the disruption at the outset. RBC staff manually entered hundreds of thousands of transactions - only catching up when the weekend volumes dropped. The timing of the error was crucial, according to Martin Lippert, Chief Information Officer at RBC, "If it had happened on a Saturday, you'd never have known about it". The problem, he said, was that the delay required to fix the error and rerun the overnight data left the system trying to run two day's transactions simultaneously, causing further delays.

The failure affected millions of individuals who either lost account balances, received duplicate or missing payments within those accounts, or had their transactions delayed. The problem had ripple effects for other financial institutions, who had some clients receive duplicate or no transfers from their employers who banked at RBC. Cascading problems included a massive e-mail scam that attempted to steal RBC client bank account information by posing as an RBC website.

RBC prides itself on its technical ability and superior redundancy. However, it may not have provided the leadership to utilize its capability. RBC is now forced to turn its attention to accountability – the bank has hired an outside firm to determine the cause of the disruption.

Activating the Plans

What Worked: A recovery plan including technical redundancy and a backup system was available.

What Failed: Plans and activation decisions did not consider the timing and volume of work required to recover, making it impossible to meet recovery objectives.

Key Quote: "If it had happened on a Saturday, you'd never have known about it"

Lesson: The best technical redundancies will not provide efficient recovery if individuals do not activate the plan.

RBC has suffered prolonged North American media attention, including gruesome stories of less wealthy individuals being charged interest bearing loans

until their account balances can be verified. The CIO's job and reputation are currently at risk, as is the reputation of the entire firm. One prominent law firm is awaiting approval to proceed with a class action lawsuit against the company.

2.4. Hewlett Packard

In March 2003, an employee suspected of having Severe Acute Respiratory Syndrome (SARS) showed up to work at the Markham, Ont. IT processing facility of Hewlett-Packard Canada Ltd., a technology solutions provider to consumers, businesses and institutions globally. The division provides IT outsourcing services to client organizations – mismanagement could affect revenue and reputation.

The York Region Health Unit was notified and after conducting an assessment upgraded the employee to probable. They contacted a number of people in the building and advised them to quarantine themselves (including visitors and deliveries).

Executives told designated employees to stay home until further notice from health authorities and turned off security cards to deny them access. A 12-person emergency staff kept the Markham operation running for the 10 days of quarantine. Normally the operation requires 60 people.

Communication

What Worked: Emergency response and recovery plans were in place and effectively activated.

Lesson: Communication with staff in a crisis is paramount. Because HP had complete contact information in their BCP plans, all staff were kept adequately informed.

The affected site was backed up by another location, and contingent processes were in place and tested regularly. Critical services were still provided during the disruption, and normal operations were restored after the crisis.

2.5. Merrill Lynch

The Merrill Lynch headquarters were located in two of the buildings in the World Financial Center just across the road from the World Trade Center in New York City. These buildings, combined with their other office facilities in the New York area, translated to almost 9,000 displaced employees on September 11th.

The 19 members of the business continuity team at Merrill Lynch were responsible for ensuring the business continuity program was comprehensive and addressed more than just government regulations. This team was responsible for making sure that the firm followed adequate Business Continuity Planning (BCP) controls. They also mandated the plans be tested twice each year and that they be developed for a worst-case scenario – in this case, six weeks without access to the primary facility at the worst possible time for an outage.

Paul Honey, Director of Global Contingency Planning,

Exercising and Testing

What Worked: Regular simulation exercises.

Key Quote: "extensive testing and upgrading of the contingency plans (kept) Merrill Lynch on track during this chaotic event."

Lesson: Regular exercises imbue staff with the ability to think on their feet in the midst of chaos.

credits “extensive testing and upgrading of the contingency plans with keeping Merrill Lynch on track during this chaotic event. The firm had recently tested their plans via a scenario very equal in impact to the terrorist attacks. The test was not a terrorist attack…, but it was a disaster of similar scope and had an equal impact on the business.”[3] This simulation of a natural disaster prepared the team and staff members to deal with the logistical, technological, and people-related issues that they faced in the aftermath of the September 11th attacks.

In addition to highlighting the need for exercising the plan, the Merrill Lynch experience also outlined the necessary steps to successfully recovering the business after a significant business disruption. They activated a well-documented continuity plan, initiated the crisis management and emergency response procedures immediately, and focused on the people and communication efforts before worrying about operational and financial concerns.

The corporate response team was comprised of cross-functional representation from the major service organizations that were instrumental in assessing the situation and prioritizing the next steps. Merrill Lynch had backup data centers outside of the immediate area as well as a contract with a hot site provider as an additional contingency. Employees already knew what a command center was and what they were supposed to do if disaster struck. Employees also knew how to contact their managers, and key employees carried wallet cards that told them whom to call and when. A number of the employees were able to work from home, and some of the work was transferred to other offices. There was a clear focus on people and communications issues as the first priority in the recovery effort.

2.6. Nokia

“In March 2000, a lightening bolt caused a blaze at a Phillips Electronics factory in Albuquerque, NM. Ten minutes after the strike the fire was out of control, and far away in Scandinavia this small event sparked a corporate crisis that shifted the balance of power between two of Europe's largest electronics companies.”[4]

Ericsson and Nokia both relied on a steady supply of computer chips from this factory to continue production of their respective mobile phones. Nokia noticed "a glitch in its supply of computer chips" and immediately launched its business continuity plan. By the time Ericsson noticed what was happening, Nokia had initiated contracts with most of the alternate suppliers. The result was a $600M revenue loss for Ericsson, along with a 50% reduction in market share. [4]

The response by Nokia was a result of “sound corporate governance and executive stewardship; and without it, a company risks losing large amounts of revenue and market share.”[5] The fact that Nokia had already

Supply Chain

What Worked: Knowing how to react to a supply chain crisis.

What Failed: Ericsson was unable to react in time.

Key Quote: The response by Nokia was a result of “sound corporate governance and executive stewardship; and without it, a company risks losing large amounts of revenue and market share.”

Lesson: Know what your key vendors’ continuity plans include, and have alternate vendors identified in case those plans fail.

[3] Ballman, Janet
[4] www.contingencyplanning.com/article_index.cfm?article=523
[5] Power, Peter G.

determined what it needed to do if its supply of computer chips was interrupted gave it the advantage it needed to ensure the continuity of its production processes.

2.7. Texas Instruments

On Monday, January 16th, 1995, at 2:51pm, an earthquake struck Kobe, a city 300 miles outside of Tokyo. Measuring 7.2 on the Richter scale, the earthquake disabled the Kobe-based KTI computer center, whose systems support the semi-conductor plant's automated manufacturing plant. This plant manufactures memory chips for Texas Instruments, which were a critical link in the organization's supply chain. Texas Instruments learned that the entire region had lost electrical power, which would be out for seven days.[6]

Texas Instruments (TI) activated their Business Continuity Plan. In another plant in Miho, TI had recently upgraded their systems, and had kept the original as a backup. Several recovery teams worked together to restore the Kobe manufacturing processes in Miho. Within two days, the plant was operational, saving $8 million USD of work in progress.[7]

Texas Instruments also had selected two software tools to assist in the business continuity planning process. Taylor's group uses "SunGard's Total Recovery Planning tool, and the Living Disaster Recovery Planning System from Strohl Systems."[8]

Critical Processes

What Worked: Correctly classified systems and processes.

Key Quote: "Not all business activities are critical. And not all systems require the same level of planning."

Lesson: A regularly updated Business Impact Analysis will identify your most critical activities.

According to Ben Taylor, Texas Instrument's manager of contingency and disaster recovery planning, "Not all business activities are critical. And not all systems require the same level of planning." TI has a steering committee that assesses the importance of various systems in a recovery effort. These fall into three categories: A "critical" system must be restored within 48 hours, ; a "secondary" system must be restored within 72 hours, and an "inconvenience" system need not be restored.[9] Fortunately for Texas Instruments, the processes in the Kobe plant were correctly classified and adequately protected.

[6] "When Disasters strike distributed systems", Software Magazine; Englewood; Sep 1995; Hanna, Mary.
[7] "When Disasters strike distributed systems", Software Magazine; Englewood; Sep 1995; Hanna, Mary.
[8] Ibid.
[9] "When Disasters strike distributed systems", Software Magazine; Englewood; Sep 1995; Hanna, Mary.

2.8. Cantor Fitzgerald

Cantor Fitzgerald[10] is an international brokerage firm responsible for transacting 200 billion dollars of securities a day, or $50 trillion dollars a year, more than the American and New York Stock Exchanges and the Nasdaq combined.[11] Of Cantor Fitzgerald LLP's more than 2,300 employees worldwide, about 1,000 occupied floors 101 through 105 of the World Trade Center's north tower. On September 11th, 658 employees perished in the terrorist attacks, and their offices were destroyed. Cantor Fitzgerald's survival of September 11th contains important lessons for those wanting to learn about business continuity. Cantor's story is particularly relevant for the following reasons:

- **Financial services**: Cantor Fitzgerald is a financial services firm that lost its headquarters. Most organizations can relate their Treasury or Marketing functions to the operations lost, and can observe the risk of losing critical head-office functions.
- **Magnitude**: Cantor Fitzgerald suffered the greatest loss in the largest terrorist attack on US soil. Other organizations can learn from the broad range of issues that this company faced and managed with different levels of success.

This section of the white paper discusses how Cantor Fitzgerald was able to survive, and what lessons can be taken from their experience.

For Howard Lutnick, CEO of Cantor Fitzgerald, September 11th was a particularly traumatic day. Not only did he lose more than half of his head office employees, but among those were his brother Gary Lutnick, and best friend and Vice Chairman Doug Gardner. Lutnick himself survived only because he was taking his son to his first day of kindergarten.

The company's initial response was to determine who was alive. Surviving executives met at Lutnick's home and were provided a "copy of a year-old company phone list. They started the difficult job of calling households, talking to wives and husbands to see if the name on the list somehow made it out – or if the person was home sick, or away on vacation."[12] Their calls provided "false moments of hope"[13] to surviving spouses waiting for word of their loved ones' safety. They also set up a crisis center for families at a nearby hotel.

Around Lutnick's dining room table, executives went through the divisions to determine which ones they would be able to salvage. The following conclusions were made about the survival rates of employees in each of Cantor's business units:

- Municipal Bonds: 1 out of 36 survived
- Corporate Bonds: 4 out of 86

---

[10] Cantor Fitzgerald also owns and shared office space with TradeSpark and eSpeed. **TradeSpark**, L.P. is a limited partnership comprised of 8 major investors. This group includes Cantor Fitzgerald, eSpeed, Inc., Coral Energy, Dominion, Koch Energy Trading, Inc., TXU Energy Trading, a subsidiary of TXU, and Williams Energy Marketing and Trading Company. Active TradeSpark marketplace participants include other major energy companies and including: Dynegy Inc. and Entergy. **eSpeed Inc.**, a subsidiary of Cantor Fitzgerald, is the leader in developing and deploying electronic marketplaces and related trading technology that offers traders access to the most liquid, efficient and neutral financial markets in the world. eSpeed operates multiple buyer, multiple seller real-time electronic marketplaces for the global non-equity capital markets, including the world's largest government bond markets and other fixed income marketplaces.

[11] On Top of the World, Tom Barbash, 7

[12] Tom Barbash, *On Top of the World: Cantor Fitzgerald, Howard Lutnick and 9/11: a story of loss and* renewal, Harper-Collins, 2003, page 20

[13] Barbash, 21

- Equities: 16 out of 140
- Mortgage-backed securities: 2 out of 36
- Foreign Exchange Forwards: 1 out of 8
- TradeSpark Energy Trading: 4 out of 44
- Human Resources: 1 out of 9
- Repos: 0

Missing leadership exacerbated the problems. Among the fallen were the two Vice-Chairmen, the CFO, Corporate development director, National Sales Manager, Head of Nasdaq trading, Head of Agencies, Head of Mortgages, and the Head of Product Development. With some hesitation, the executives decided to exit Corporate Bonds, Mortgage backed securities, and Foreign Exchange. Lutkin explained that he was fighting his ego, "because part of me wanted to keep it all and show that we could turn it all around – save everything. But I knew what the risks were – that if we tried to save everything, we could lose the whole company."[14]

They responded to the crisis to the best of their ability without plans that forecasted such a massive disaster. Fortunately, the existing information technology had some redundancies. In some areas, the firm had secondary and tertiary system redundancies. Cantor's data lines had been duplicated at Verizon's hub, but they were only a few blocks from the Trade Centre, and were ruined. Fortunately, they were also backed in a Rochelle Park, New Jersey, disaster recovery site[15]. This added distance provided enough redundancy to build parts of their systems in New York. Even so, technology teams were forced run some systems from the London office. [16]

Technology & Facility

What Worked: Cantor owned an alternate hot-site for disaster recovery.

What Failed: Over dependence on telecommunications for some critical processes and "redundant" servers in same physical location.

Key Quote: "The previous disaster-recovery plan was based on a co-location plan … but Giaccone [architect of the disaster recovery plan] pushed for more."[7]

Lesson: Have an alternate site that mirrors all of the critical systems.

The company was able to resume trading on Thursday September 13th from its backup site in New Jersey, but there were significant business challenges caused by the disaster. Competitors were vying for the company's business. Morgan Stanley Dean Witter ran a full-page ad, signed by its chairman, Philip Purcell, in the Wall Street Journal, stating that all of their clients' assets were safe. The ad was placed to "tell the world that it should do business with Morgan Stanley … because people will want to do business with a company that is functioning on all cylinders."[17] BrokerTec distributed a press release titled "BrokerTec Gains Bond Market Share as Tragedy Begets Opportunity", suggesting it had "gained prominence it may not surrender." [18]

In addition to competition issues, the difficulty of clearing transactions led to cash flow problems. Failure to settle the trades can lead to significant financial implications, because "if you don't get paid for the stocks you've sold and your own cash is flying out the door, the bank can shut you down, and then you're through. And you won't just lose money then. Even the most loyal workers need to make house payments. All those firms that watched Cantor grab their best brokers and

[14] Barbash, 53
[15] Barbash, 55
[16] The Key Quote in the caption about Giaccone is from Baseline, October, 2001, "Forty-Seven Hours", by Sean Gallagher.
[17] Barbash, 43
[18] Barbash, 62

traders over the years will hardly feel guilty about taking a few of them back."[19] Aware of their fragile position, Cantor's bank, JP Morgan Chase, pressured Cantor about its loans. The bank was sympathetic, but told Lutkin the loans would need to come down, or at least stabilize. The bank "didn't spell out what would happen if they didn't, the message was clear: The firm was in danger of going under."[20]

> *People*
>
> *What Worked:* People with similar skills available in London to carry out critical business processes.
>
> *What Failed:* Out of date phone lists and insufficient preparation for relief and compensation of fallen employees.
>
> *Key Quote:* Late planning "is such a huge waste of my time. Should have happened much, much earlier."
>
> *Lesson:* Successful continuity planning incorporates more than just technology.

Lutkin was forced to make a decision to stop paying the salaries of fallen employees. Instead, the company committed to pay for 10 years of healthcare, $100,000 per family of life insurance, $45 million in bonuses (totalling 175 million).[21] Plus, the company committed to distributing 25% of the profits for five years to the families. However, the communication was not sufficient for such a complex plan, and media and families lashed out at the company. One spouse was quoted as saying "It didn't have to be so brutal … they could have given us at least two weeks to grieve without having to think that our husbands were gone." A reporter described Howard as "aggressive, ambitious, ruthless, and willing to step on or over anyone to get what he wants." The O'Reilly Factor with Bill O'Reilly sensationalized the bad press on a nightly basis, which had a "devastating effect on the business and on Howard's public persona."[22] The negative press "decimated the relief effort, hurt the equities business and eSpeed's stock."[23] The resulting turmoil took much of the leadership's energy at a critical time.

Fear of more negative publicity caused Lutkin and his HR experts to push late into the night to finalize the plan and get it to the families and to the press quickly. Issues like bonuses and unused vacation time plagued the discussion, and were complicated by the lost divisional heads and their records. The discussion was not just about what to include, but how to present the various aspects of the plan. "Three hours into the discussion, on the night of his brother's memorial, with ten people in his dining room with papers and calculators out, and after four nights of endless circular squabbles about each issue, Howard says 'We waste *so much time* with this. This is such a huge waste of my time. Should have happened earlier. Much, much earlier.'"[24]

Tom Trillo, 45 year-old head of operations, preferred less communication with the media, to avoid over-promising to key stakeholders. "Every day at three o'clock I get to talk to the GSCC and work out where we are with our positions on the Street and how much cash we have and why we aren't clearing trade to the levels we used to. And at four o'clock I get the pleasure of talking to the bank. And say 'I need you to lend me another eighty million dollars unsecured overnight.' 'Okay, Tom,' they say. 'So what are you doing to do for us tomorrow? How are your deliveries going?' And at five o'clock, I get to talk to the head of regulatory reporting at the SEC, right? And I get to tell him we're not going to file our reports on time as regulated by the SEC because we don't have our systems to

[19] Barbash, 55
[20] Barbash, 44
[21] Barbash, 177
[22] Barbash, 133
[23] Barbash, 143
[24] Barbash, 134

where they need to be. And, yeah, could you cut me some slack? So that was my day, every day – every day, the level of stress I was under in talking to the depositories, the banks, and the regulators to try and convince them that we're okay."[25]

On the day trading resumed, Cantor's customers flooded them with business, almost killing them with kindness. Cantor Fitzgerald had one of its busiest days ever. Fearing an inability to settle enough trades and cause loans to spiral out of control, Lutkin waited for the bank to call. When the bank called, they informed Lutkin that his company had delivered out just enough stocks and bonds. Since the loans had not gone up, they learned they would stay in business.[26]

The company was able to resume trading from its backup site in New Jersey. Cantor Fitzgerald has since achieved profitable operations, distributing $63 Million to the families of its fallen employees. Cantor suggests its successful recovery was due to "the remaining global staff that turned a remote facility into a North American Hub … customers that rallied to help save them … and that workers were driven by the memory of their colleagues."[27]

3. Conclusions

From these stories and others we know that successful business recovery requires several ingredients. Executives that are concerned with improving their organization's resilience should attempt to keep theses ideas alive in their company.

The first ingredient is leadership. Before a disaster, a lack of leadership will cause a plan to never be developed. At the time of disaster, successful recovery requires a team of leaders/managers to assess the situation, prioritize what must be done, coordinate the activities and make decisions used the resources they had available to them at the time of the crisis. They must be able to improvise and adapt as necessary, and provide quick assessment of the human impact on the business.

Companies must also be prepared and know exactly what to do when an incident occurs. They must have a plan. This plan should include a communications center and methods of communicating frequently to employees, the media, customers, vendors and other key stakeholders. The program should architect data center facilities in such a way as to ensure high availability of mission critical data and business applications. Some thought should be given to an employee relocation strategy, or combining alternatives such as alternate sites and remote working. The plan will include ways to obtain temporary housing, food, and transportation for relocating employees. IT will go the added mile to back up the backup site while returning operations back to the primary site. Further, the plan will build recovery plans into the operating environment as part of the operational real estate and data center strategies. John Sharp, chief executive officer of the Business Continuity Institute suggests that Business Continuity is not just about IT. BCP should take into account critical functions by looking at the "'4P's': people, process, premises and providers"[28].

[25] Barbash, 151
[26] Barbash, 61
[27] www.eSpeed.com, July, 2003
[28] "Special Report: Business Risk – Catastrophe: Are You Prepared?", Accountancy, London, Jan1, 2003, Matt Warner

The third ingredient is exercising and testing. Regular exercising will ingrain the plan to those individuals who will be required to rise to greatness should a disruption occur. And regular testing of the plan will identify problems in the planning, allowing adjustments to be made.

Successful recovery also requires a company to protect what is critical, and that can change rapidly in today's environment. Companies that do a regular Business Impact Analysis to ensure they understand their operations and financial impacts, and then focus their efforts on restoring critical processes, fare the best.

Companies must focus on their people, first. Of the hundreds, if not thousands, of articles that have been written about the effects of September 11th, certain key elements are consistent throughout. Understandably, the most important lesson is the value of people to an organization, and the inherent frailty of that asset. Although most of the companies impacted by September 11th had some kind of disaster recovery plan in place, they had significantly underestimated the effect of a disaster on their workforce. As long-term impacts of the disaster were analyzed, it was found that those companies who struggled the most did so because of overwhelming staff losses.[29] Aside from the losses caused by the event itself, some people never did return to work due to the trauma they were facing, others continued to leave long after the event. The longer it takes to restore normalcy for people, the more stress they are placed under. Some people simply give up and go home.

The final ingredient in minimizing the negative impact of a crisis is luck. Corporations that fare well are often blessed with small gifts in the face of disaster, such as an unaffected alternate site, or extraordinary feats by ordinary people. There is really no way to avoid all loss in the face of a disaster, but sometimes lady luck will give you the opportunity you need to minimize that loss.

Of course, there are many who believe that luck happens when *preparation meets opportunity*. We will let you be the judge.

[29] Ferris, Gregory J. www.rmmag.com/

4. Appendix

#	Question	Yes	No
1.	**Plan**: Do you have a Business Continuity Plan that incorporates Process, People, Information Technology and Facility?		
2.	**Test**: Has your plan been tested, and are results of that test used to improve the plan?		
3.	**Action**: Does your organization have a dedicated crisis management operations center and backup facility for incident command and communications functions in the event of a serious business disruption?		
4.	**Leadership**: Does your organization have BCP program sponsorship from the CEO and the executive team?		
5.	**Leadership**: Does your organization have a dedicated team responsible for business continuity planning across the corporation?		
6.	**Leadership**: Does your organization have key personnel identified and trained to respond to a corporate crisis?		
7.	**Protect what is critical**: Does your organization understand what its most critical functions are, what the impacts of those functions are to the organization, and what is needed to complete those functions?		
8.	**People:** Does your organization have sufficient distribution of its human assets?		
9.	**People:** Does your organization understand how it will provide relief to employees and their families in the event of a disaster?		
10.	**People:** Does your organization have well-planned crisis management and emergency response plans that ensure the safety of employees in the event of a disaster?		

Bibliography

Air Canada, 2003 3rd Quarter Report. http://www.aircanada.ca/about-us/investor/pdf/2003_q3.pdf

Ballman, Janet, *Merrill Lynch Resumes Business Critical Functions Within Minutes of Attack*, Disaster Recovery Journal, Summer 2001, www.drj.com (July 19, 2003).

Barbash, Tom, *On Top of the World*, 7

Cruickshank, Doug, *The road to recovery: September 11 stripped us of our innocence, forcing corporations to recognize that disaster planning is a business necessity*, CA Magazine, v. 135(7) S'02 pp 20-23.

Ferris, Gregory J., *Response and Recovery at Morgan Stanley*, Risk Management Magazine, New York, v. 49(12), Dec. 2002, http://www.rmmag.com/ (July 4, 2003).

Greenberg, Jeffrey W., *September 11 – A CEO's Story*, Harvard Business Review, October 2002, pp 58-64.

Hagg, Andy, *Back To Work*, November 2001, pp 14-17.

Hanna, Mary, "When Disasters strike distributed systems", Software Magazine; Englewood; September 1995.

Hiles, Andrew and Barnes, Peter, *The Definitive Handbook of Business Continuity Management*, John Wiley & Sons, Ltd., Chichester U.K., 2001.

Kaufman, Neil; Pullara, Jack; Davenport, Mary Grace; Thompson, Chris, *Insights from the Events of September 11th: Is your organization prepared?*

McArthur, Keith, "Blackout slams Air Canada", *Globe and Mail*, August 16th, 2003. http://www.theglobeandmail.com/servlet/story/RTGAM.20030816.wxrairl0816/BNStory/Business/

Messmer, Ellen, *IT pros share painful lessons*, Network World, July 2002 (www.nwfusion.com (July 17, 2003)

O'Brien, Jennifer, *Life-saving business strategies get low priority*, Computing Canada, v.25(12) Mr 26'99 pp 11,13.

Power, Peter G., *Manage a Crisis, Don't Recover from Disaster*, Contingency Planning Magazine website, January 2003, pp22-26, www.contingencyplanning.com, (June 27, 2003).

Reguly, Eric, "RBC must restore confidence", The Globe And Mail, Tuesday, June 8, 2004.

Reuters News Agency, with files from Bloomberg News, *'My view of business is different': Cantor CEO*, New York, Friday, September 14, 2001.

Saunders, John, "RBC Blames Human Error", *The Globe And Mail*, Thursday, June 10th, 2004.

Risk Management Society Publishing Inc., *Response and recovery at Morgan Stanley*, New York, Dec 2002.

Toigo, John William, *Storage Disaster, Will you Recover?*, Network Computing website, March 5, 2001, http://www.networkcomputing.com/1205/1205f1.html, (July 7, 2003).

Warner, Matt, *"Special Report: Business Risk – Catastrophe: Are You Prepared?"*, Accountancy, London, Jan 1, 2003.